

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. Please cancel claims 1-10 and 27-30 as follows:

Listing of Claims:

1-10. (Canceled)

11. (Previously Presented) A method for providing access to computer resources on a computer system, comprising:

under control of a client system,

providing user information to a server system, the user information including authentication, authorization, and credit information for a user of the client system;

receiving from the server system, a token including encrypted information generated from the user information provided by the client system;

a remote application manager component; and

at least one computer resource, each computer resource being encrypted and the particular computer resources received being determined from the authorization information contained in the provided user information;

under control of the remote application manager component on the client system,

decrypting at the client system the token in response to a request to initiate execution of one of the computer resources;

authenticating the user of the client computer system;

verifying whether the user is authorized to use the requested computer resource;

verifying whether the user has sufficient credit contained in the token to use the requested computer resource;

when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the requested computer resource; and

monitoring the usage of the executing computer resource and providing a notification when the monitored usage has exceeded the user's credit.

12. (Original) The method of claim 11 wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token.

13. (Original) The method of claim 11 wherein a request to initiate execution of one of the computer resources comprises clicking on an application icon.

14. (Original) The method of claim 11 wherein the token and each computer resource have been encrypted using the public key encryption methodology.

15. (Original) The method of claim 11 wherein each computer resource comprises an application module.

16. (Original) The method of claim 15 wherein each application module comprises an entire executable application program that is stored in encrypted form on the computer system.

17. (Original) The method of claim 11 wherein monitoring the usage of the executing computer resource comprises monitoring how long the user has been using the computer resource.

18. (Original) The method of claim 11 wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted.

19. (Previously Presented) A method for providing access to computer resources on a computer system including client and server systems, comprising:

- under control of a client system,
- providing user information to a server system, the user information including authentication, authorization, and credit information for a user of the client system;
- under control of a server system,
- generating a token including encrypted information generated from the user information provided by the client system;
- sending the token to the client system;
- sending a remote application manager component to the client system;
- sending at least one computer resource to the client system, each computer resource that is sent being encrypted;
- under control of the remote application manager component on the client system,
- initiating execution of the remote application manager component in response to a request to initiate execution of the computer resource;
- decrypting at the client system the token and authenticating a user of the client computer system;
- verifying at the client system whether the user is authorized to use the computer resource;
- verifying at the client system whether the user has sufficient credit contained in the token to use the computer resource;
- when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the computer resource; and
- monitoring the usage of the executing computer resource at the client system and providing notification when the monitored usage has exceeded the user's credit.

20. (Original) The method of claim 19 wherein the token is stored on a smart card that the remote application module component accesses to retrieve and decrypt the token.

21. (Original) The method of claim 19 wherein a request to initiate execution of one of the computer resources comprises clicking on an application icon.

22. (Original) The method of claim 19 wherein the token and each computer resource have been encrypted using the public key encryption methodology.

23. (Original) The method of claim 19 wherein each computer resource comprises an application module.

24. (Original) The method of claim 23 wherein each application module comprises an entire executable application program that is stored in encrypted form on the computer system.

25. (Original) The method of claim 19 wherein monitoring the usage of the executing computer resource comprises monitoring how long the user has been using the computer resource.

26. (Original) The method of claim 19 wherein providing a notification when the monitored usage of the opened computer resource has exceeded the credit comprises displaying a visual message to the user instructing the user to save his work and indicating his credit has been depleted.

27-34. (Canceled)